



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/787,648	03/20/2001	Gerrit Roelofsen	PTT-111(4025	5973
7265	7590	01/11/2006	EXAMINER	
MICHAELSON AND WALLACE PARKWAY 109 OFFICE CENTER 328 NEWMAN SPRINGS RD P O BOX 8489 RED BANK, NJ 07701			DERWICH, KRISTIN M	
			ART UNIT	PAPER NUMBER
			2132	
DATE MAILED: 01/11/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/787,648	Applicant(s) ROELOFSEN ET AL.	
	Examiner Kristin Derwich	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 October 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 33-67 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 33,34,36,50-67 is/are rejected.
- 7) ☐ Claim(s) 35 and 37-49 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 March 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 33-67 are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 24, 2005 has been entered.

Response to Arguments

3. Applicant's arguments filed October 24, 2005 have been fully considered but they are not persuasive. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., further explanation of what "compensating influence of the auxiliary values" encompasses, a more specific description of "invertability") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Allowable Subject Matter

Art Unit: 2132

1. Claims 35, and 37-49 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Hereafter patent literature that is referenced as prior art will be cited by column and line number in the form of (column number:line number range). For example, the citation (6:23-27) refers to lines 23-27 of the 6th column in the reference.

1. Claims 33 and 34 rejected under 35 U.S.C. 102(b) as being anticipated by Wood, U.S. Patent No. 5,003,596.

As per claim 33:

Wood discloses a method for cryptographically processing data, comprising:

Feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K) (fig. 8, wherein item 104 is the data (X), item 116 represents the key (K) and items 106, 112, 114, 118, 120, 122, 126, 130, 132, 136, 138, 140 and 144 represent the cryptographic process (P) collectively).

Carrying out the process (P) in order to form cryptographically processed output data (Y) (fig 8., wherein item 146 is the output data (Y)), characterized by

Art Unit: 2132

Feeding, to the process (P), auxiliary values that mask the data (X) used in the process (P) (fig 8., wherein item 110 represents the auxiliary values that mask the data; 11:64-67, wherein transformation of the data represents masking the data), and

Compensating, by an auxiliary process, the influence of the auxiliary values on the output data (Y) (12:4-6; 31-43, wherein the mask creation is the auxiliary process).

As per claim 34:

Wood discloses a method of cryptographically processing data, comprising:

Feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K) (fig. 8, wherein item 104 is the data (X), item 116 represents the key (K) and items 106, 112, 114, 118, 120, 122, 126, 130, 132, 136, 138, 140 and 144 represent the cryptographic process (P) collectively),

Carrying out the process (P) in order to form cryptographically processed output data (Y) (fig 8., wherein item 146 is the output data (Y)), characterized by

Feeding, to a supplementary process (P*), a supplementary key (K*) in order to form the key (K) (fig. 3, wherein item 50 is the supplementary key (K*) and items 51-58 represent the supplementary process (P*) collectively and the item 59 represents the key (K)),

Wherein the supplementary key (K*) masks the key (K) used in the process (P) (fig. 3 shows the supplementary process (P*) that utilizes the key (K*) to mask the key (K)), and

Wherein the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed (6:24-31, wherein the initialization vector acts as the auxiliary key (K')) and is fed to the process which creates the key table utilizing the supplementary key (K*)).

Wood discloses a method wherein the supplementary process (P*) is in invertible process (8:8-10, 20-22, since you can work backwards to get the original plaintext, the process is invertible).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claim 36 rejected under 35 U.S.C. 103(a) as being unpatentable over Wood (U.S. 5,003,596) as applied to claims 33 and 34 above and further in view of Schneier, Applied Cryptography.

Wood substantially teaches a method of cryptographically processing data, comprising:

Feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K) (fig. 8, wherein item 104 is the data (X), item 116 represents the key (K) and items 106, 112, 114, 118, 120, 122, 126, 130, 132, 136, 138, 140 and 144 represent the cryptographic process (P) collectively),

Carrying out the process (P) in order to form cryptographically processed output data (Y) (fig 8., wherein item 146 is the output data (Y)), characterized by

Feeding, to a supplementary process (P*), a supplementary key (K*) in order to form the key (K) (fig. 3, wherein item 50 is the supplementary key (K*) and items 51-58 represent the supplementary process (P*) collectively and the item 59 represents the key (K)),

Wherein the supplementary key (K^*) masks the key (K) used in the process (P) (fig. 3 shows the supplementary process (P^*) that utilizes the key (K^*) to mask the key (K)), and

Wherein the supplementary process (P^*) comprises a cryptographic process to which an auxiliary key (K') is fed (6:24-31, wherein the initialization vector acts as the auxiliary key (K') and is fed to the process which creates the key table utilizing the supplementary key (K^*)),

The supplementary process (P^*) is performed only if the data (X) is performed only if the data (X) has predetermined properties (5:54-58).

Wood fails to teach the data (X) being fed to the supplementary process (P^*) in addition to the auxiliary key (K^*). However, Schneier discloses a process called whitening where the supplementary process is an XOR combinatory process and both the data and some key material are fed to the XOR process before executing the primary process, in this case, DES (Schneier, 15.6). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to feed the data and the key to a supplementary XOR process in order to hide plaintext patterns, which is similar to masking, as stated in Schneier (pg 363).

3. Claims 51, 57 and 67 rejected under 35 U.S.C. 103(a) as being unpatentable over Wood (U.S. 5,003,596) as applied to claims 33 and 34 above and further in view of Miyano (U.S. 5,442,705).

As per claims 51 and 57:

Wood fails to teach a method wherein the process (P) comprises DES. However, Miyano discloses a method wherein DES is utilized as the process (P) (2:47-53).

Art Unit: 2132

4. Claims 50, 53-56, 59-61 and 66-67 rejected under 35 U.S.C. 103(a) as being unpatentable over Wood (5,003,596) as applied to claims 33 and 34 above, and further in view of Bouricius et al. (Bouricius), U.S. Patent No. 4, 302, 810).

As per claims 50, 56 and 62:

Wood fails to teach a method wherein the data (X) comprises identification data of a payment means (1) and the processed data (Y) forms a diversified key. However, Bouricius discloses a method wherein a secure transmission to a host machine of a transaction message describes a financial transaction between a person and a retailer (3:53- 57).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use identification data of a payment means to produce a diversified key in addition to using a circuit to carryout a cryptographic method, a payment card and a payment terminal in combination with the cryptographic block cipher as disclosed by Wood in order to prevent eavesdroppers on the transmission lines from obtaining any information which could later be used for fraudulent, illegal, or any other purposes as stated by Bouricius (2:8-12, 4:17-23).

As per claims 53, 59 and 66:

Wood fails to teach a circuit for carrying out a method for cryptographically processing data. However, Bouricius discloses a method which includes means for an encryption circuit to carryout an encryption processes (5:37-39).

As per claims 54, 60 and 67:

Wood fails to teach a payment card provided with a circuit. However, Bouricius discloses a method which includes an electronic funds transfer card (2:26).

As per claims 55 and 61:

Art Unit: 2132

Wood fails to teach a payment terminal provided with a circuit. However, Bouricius discloses a portable transaction terminal device (2:27).

5. Claims 31 and 32 rejected under 35 U.S.C. 103(a) as being unpatentable over Wood (U.S. 5,003,596) in view of Miyano (U.S. 5,442,705) as applied to claims 22 and 27 above, and further in view of Heer et al. (Heer), U.S. Patent No. 6,028,933.

As per claims 51, 58, 63 and 64:

Wood and Miyano fail to teach a method wherein the DES process is triple DES. However, Heer discloses a method wherein triple DES is utilized.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize triple DES in a cryptographic process as disclosed in Wood and Miyano because as stated in Heer, triple DES provides twice the encrypting power of a pure DES encrypting process making it much more secure (2:62-67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

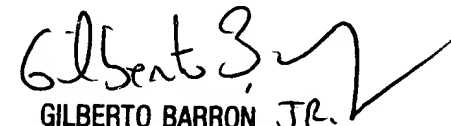
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


KMD

Kristin Derwich
Examiner
Art Unit 2132


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100